Security Advisory 2021-014

Vulnerabilities in Microsoft DNS Server

March 10, 2021 — v1.0

TLP:WHITE

History:

- *10/03/2021 — v1.0 – Initial publication*

Summary

On the 9th or March 2021, Microsoft released several security advisories for Windows DNS Server. Five of those vulnerabilities would allow a remote attacker to execute code on the target if the DNS service is exposed [1, 2, 3, 4, 5]. One of them is considered as critical by Microsoft (CVE-2021-26897) [1].

No proof-of-concept or ongoing exploitation of these vulnerabilities are public yet. However, because of the potential impact of the vulnerabilities and the fact that to be vulnerable, a DNS server would need to have dynamic updates enabled, which is the default configuration, it is highly recommended to **apply the patches as soon as possible**.

Enabling Secure Zone Updates would protect from attacks on public-facing interfaces, but not from an attacker with a foothold on the network (domain-joined computer).

Technical Details

All five vulnerabilities have the same descriptions by Microsoft, however McAffee provided technical analysis for CVE-2021-26877 and CVE-2021-26897 [6].

The vulnerability identified as critical by Microsoft (CVE-2021-26897) is triggered when many consecutive Signature RRs Dynamic Updates are sent to the DNS server leading to a write on the heap when the updates are combined into base64-encoded strings before writing to the zone file.

The other analysed vulnerability (CVE-2021-26877) is triggered when a zone is updated with a TXT RR that has a `TXT length` greater than `Data length`.

Affected Products

- Windows Server 2016
- Windows Server 2019
- Windows Server 2012 (including R2)
- Windows Server 2008 (including R2, R2 SP1 and R2 SP2)
- Windows Server, version 2004
- Windows Server, version 1909
- Windows Server, version 20H2

To be exploitable, the server needs to have the DNS role enabled with Dynamic Update enabled (default configuration).

Recommendations

Apply the patches as soon as possible [2]. It is recommended to prioritise the updates on Internet-facing Windows DNS Servers.

Mitigation

Two mitigation can be done in order to limit the exploitability of the vulnerabilities:

- Deactivating Dynamic Update feature.
- Enabling Secure Zone Updates to limit the exploitability.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26897

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26895

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26894

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26893

[5] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26877

[6] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/seven-windows-wonders-critical-vulnerabilities-in-dns-dynamic-updates/